

The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes

Gary T. Marx | MIT



After the Boston marathon bombings, citizens and the private sector provided police with thousands of tips, sound, and video images—and we saw the subsequent swift identification of the two suspects. Such engagement isn't new. But we've also seen a rush to judgment by citizen cybervigilantes who erroneously identify and publicize information on people who turn out not to be suspects. State retrenchment in the provision of services—given the economy—and new security, crime, and other risks (some bordering on moral crusades and even moral panics), along with the appearance of new technologies for communication and analysis, have led to increased appeals by police to citizens for help.

However laudatory the goal, there's a potential collision between the 18th century belief in policing as an integral aspect of public civic virtue in which citizens have a duty to actively engage in the maintenance of liberty¹ and the danger of creating of what Joshua Reeves refers to as “the ambiguated citizen-officer-suspect ... undeterred by legal restraints and other judicial obstacles. ... Co-workers and neighbors do not need a warrant to monitor and record your activities, deem them ‘suspicious’ and submit their findings, whether to the police or the public.² So what roles are available to the public as technology gathers more and more information about each of us? Under

what conditions do various forms of public support for law enforcement help or hinder public order and the creation of the good society?

It's easy to illustrate how quickly change is occurring by looking at the different roles information technology played in 1994 and 2011 in response to hockey riots after losses by the Vancouver Canucks. Before the advent of new information technologies, the ability of police to identify suspects and to document violations was labor intensive and episodic. After a 1994 riot, police assembled and edited news clips and made them available in kiosks around Vancouver. Citizens were encouraged to view the clips and identify anyone they recognized. In 2011, similar images appeared on Facebook rather than at kiosks. Through what Chris Schneider and Daniel Trottier call “crowd-sourced policing,” online users posted text, images, and sound without police prompting to a Facebook page called “Vancouver Riot Pics: Post Your Photos” and to another website called “Naming and Shaming.”³ Rather than going to a kiosk for data, the data now came to the citizen.

In the Boston bombing, the carefully described uses and misuses of information technology in identifying the perpetrators have helped surface broader societal issues.⁴⁻⁶ In this article, I examine some of the new opportunities and risks that computers and related communication tools bring to social control

efforts and some implications for issues of justice, liberty, privacy, and community. No matter what's new here, national security, police and criminal justice grow out of, and are encapsulated in, settings that portage enduring cultural continuities, trade-offs, and value conflicts.

Not by Technology Alone

In spite of the rapid expansion of signals intelligence in recent decades and developments in related surveillance technologies, September 11, 2001, and the Boston bombings make it clear that the cherished goal of many engineers to “get the humans out of the loop” is impossible and unwise.

Of course, much contemporary data collection is involuntary, unseen, and automated, seemingly naturally folded into routine activities such as driving a car or using a credit card, computer, or telephone; with the oncoming Internet of Things, clothes, medical devices, and household appliances will soon report back as well. Myriad passive, soft surveillance sensors based on motion, heat, sound, scent, and location provide data. Some, such as communications metadata, provide information on other parties who need not consent to this provision. But as readers of this magazine know, data aren't information, and with vast collection volumes, the ratio of signal to noise is far from useful. These problems are compounded when the needle wants to hide in the haystack or disguises itself as a button.

The police in Boston used a variety of sophisticated soft- and hardware techniques in the search for those responsible for the crime, including facial recognition techniques, dome cameras, explosive ordnance disposal units, forward-looking infrared cameras, flashbang devices that disorient, and probably other technologies that haven't become public. But regardless of the advances we've made in gathering so

much information, the data available to the state (or any organization, regardless of its size and technology) are greatly restricted by the logistical limits of space, time, and scale as well as by social and legal protections and local cultural meanings that may be unknown. This situation is even truer for clandestine matters.

In spite of clever sleuthing and the fancy forensics popularized in the mass media, a key factor in learning of and solving a goodly proportion of cases is input from citizens, be they victims, disinterested volunteers, people relating to police as informers, or individuals acting independently of police. This human support is rich in potential but fraught with risks.

A Little History

Ears to the ground and some warping (or at least inequality) of information flows as a result of social stratification are features of all societies. Gossip is a means of social control in traditional societies. In medieval Venice, citizens could anonymously inform on their neighbors' misdeeds by dropping notes into the mouths of snarling stone lions and gargoyles (called the “mouths of truth”) in public buildings. Similarly, Sherlock Holmes put to good use the sealed letters slid under his door. Hotlines and milk carton requests for help are today's equivalent.

Using citizens to extend the eyes and ears of police shares elements with the Franken pledge system of mutual support and responsibility seen in England during the Middle Ages, although that involved penalties for noncooperation. A later, more voluntary, British tradition of “watch and ward” and “hue and cry” expected all citizens (within a jurisdiction, not just local neighborhood or kin group, as in earlier centuries) to join an ad hoc manhunt after a crime occurred.⁷

In the early 19th century, the

British created a “low” permanently organized, local (rather than national) police system, developed in opposition to the European continent's “high,” presumably more repressive, police who served the sovereign, whether domestically or in colonial settings, not the people. Police in England were simply citizens with no powers beyond those of other citizens, dependent on the good will of those they served. The fact that the first modern British police force was unarmed reflects this community orientation. Ideally, citizens would obey the law and gladly provide information to police out of respect, not as a result of fear, coercion, or deception.

Over several centuries, the emerging ever more “professional” police force became more secretive, less community focused, and less dependent on citizens. Independence from untoward citizen pressures via politics was seen as necessary for a truly professional police department. Now, as the times have changed, elements of “hue and cry” have returned:² the intensive request for information from Boston citizens following the bombing was unprecedented, and the resulting data flood contributed to the relatively rapid discovery of information about “suspects 1 and 2,” and shortly thereafter reports of their names, if not their locations.

The turn to the public for help reflects some changes in what can be seen as either a democratically fringed, participatory society where community-minded citizens do their part or less charitably as a fearful and suspicious society where distrust is the coin of the realm and self-righteous vigilantes roam the ether and the land. To the Pinkerton's slogan “the eye that never sleeps” we can add “the ear that is never deaf” and the “digital record that never forgets.”

But however viewed, new means of communication and publicity

about new threats support more citizen involvement in security matters. Contemporary means extend the passive requests of the old “Wanted!” posters for fugitives—many requests are more open ended and vague, describing events that might happen, seeking input on suspicious circumstances and people. As such, they invite an unsettling categorical suspicion, whether across entire populations or within subgroups defined by ethnicity nationality, religion, or dress.

In regarding each other laterally, the citizen becomes both an agent of and a subject for surveillance. This involves looking carefully at others and perhaps feeling a bit paranoid or at least

uncomfortable, knowing others are looking right back. In challenging times, such as when public order is perceived to be at great risk, in a period of economic crisis and of diminished state services, citizens have a greater role to play, propelled by both civic responsibility and self-interest. Perhaps it’s prudent to be on guard at such times, but this guardedness can also bring anxiety and a weakening of community.

This can result in what cultural studies theorist Mark Andrejevic calls “survivalist individualism.”⁹

31 Flavors of Reporting: From the Specific to the General

A variety of specialized hotlines are available to report single drivers in carpool lanes, tax evaders, college cheaters, drug dealers (“drop a dime”), poachers, polluters, burn ban violators, litterers, and even potholes in the road. Beyond traditional Neighborhood Watch efforts, whose more than 50,000 groups “observe and report” and act as “eyes and ears of police,” and TV shows such as Crime Stoppers and America’s Most Wanted, new

programs have sprung up post-9/11, encouraging truckers, utility workers, taxi drivers, and delivery people to report suspicious activity. No longer restricted to post offices, requests now come through LED signs, the mass media, and disembodied voices in public transportation settings calling for vigilance. Silver Alerts encourage citizens to be on the lookout for missing people with dementia; similarly, Amber Alerts seek lost children. And children have called hotlines to

In regarding each other laterally, the citizen becomes both an agent of and a subject for surveillance.

turn in their parents for marijuana use after seeing school presentations about the dangers of drugs (<http://web.mit.edu/gtmarx/www/when.html>). Yet other unfocused requests seem unduly broad. In Portland not long ago, a billboard asked, “Do You Know Something the Sheriff of Multnomah County Should Know?” In 2010, following a Department of Homeland Security initiative, many Wal-Mart shoppers at the checkout stand saw a video commercial in which DHS head Janet Napolitano observes, “Homeland security begins with hometown security. If you see something suspicious in the parking lot or in the store, say something immediately. Report suspicious activity to your local police or sheriff. Thank you for doing your part to help keep our hometown safe.”

Often left vague is just what and who ought to count as suspicious, other than unattended packages. The message is that we’re a community, and we all have a role to play. Rather than simply being bystanders expecting authorities to act, we too have a responsibility. The ease of reporting on others also extends to

individuals reporting on themselves in what has become a self-monitored society.

This notion of volunteering information as good citizenship or patriotism is also increasingly seen in other contexts in which individuals are asked to waive certain rights for the greater good or some benefit. In the US Department of Justice’s “Watch Your Car” program, for example, car owners place a decal on their vehicles, inviting police anywhere in the US to stop the car if driven late at night. This is intended to serve as an anti-theft means and also to track misuses of the car. Also as an anti-theft device, in some cities, taxis not only transmit video images, which passengers consent

to by seeing a notice when they enter the cab, but also invite police to stop them without cause.

Frequent requests for service evaluation from hotels, conferences, teachers, banks, and credit card companies are a further strand of the tilt toward citizen input. Consider the truck signs that ask, “How am I driving?” or an airline that requests travelers to report a good, rather than a bad, employee. Such bottom-up and/or lateral communication along with “reality” television programs and social media form part of an emerging culture of surveillance and revelation that is increasingly taken for granted. Along with this, although not equivalent, is a reciprocal cat-and-mouse culture of dissimulation and concealment. When police pose as Facebook “friends,” we see yet another example of the state’s absorption of personal data.

There are a variety of legislative and program supports for citizen and organizational reporting and other forms of engagement:

- stand your ground laws, subpoenas, and grand jury investigations;
- the US Federal Witness Protec-

tion Program, which provides relocation and a new identity to informers;

- federal cabinet agencies' hotlines for citizens to report instances of fraud and abuse;
- legislative and judicial protections for whistle-blowers;
- a 2008 law that retroactively immunizes telecommunications companies from legal liability in providing data to the government;
- legislation in the US and England that seeks to establish the conditions under which the state can access social media data; and
- a proposed congressional See Something, Say Something act to protect citizens who report suspicious activity.

There are far fewer supports to protect against frivolous, malicious, erroneous, and harmful reports by fellow citizens, although there are the hard-to-prove privacy torts that can be brought to a civil court.

Public sex offender registries are distinct from direct requests from authorities but are related to the weakening of a type of police-citizen information border that previously existed. Before, such information wasn't available or could only be seen by going to a government office, but today, many crime reports are available online. In some communities, concerned parents scan registries for names and addresses of offenders and circulate them in postings on neighborhood networks. With the ease of such precise identification, the appearance of vigilante action from defamation to harassment to murder isn't surprising. Recently, a suspect went through the Jonesville, South Carolina, sex offender registry and created a list of targets to kill; he was arrested after the first killing.¹⁰ There's a case for making some kinds of criminal justice records publicly available (if not necessarily a mandate to make them

instantly accessible). But as a Jonesville resident noted, "We've all done something in our past, and nobody wants someone to show up with a gun and play God."

The Public as Partner

As technical developments join mounting concern over terror and crime, the state is becoming increasingly covetous in its desire for information, even as it can be overwhelmed by it. The systems for direct citizen input are expanding, so it's becoming easier for self-appointed sheriffs to report on anyone, anywhere. Think of the new potential Google Glasses will bring to quietly record sound and images and then anonymously post them on the Internet or send them to the police. There is even a free app for easy reporting: (<https://play.google.com/store/apps/details?id=susp.ac&hl=en>)

Relative to Europe, the US has more formal public and private programs for involving citizens in information gathering and less ambivalence toward (and suspicions of) such efforts. This attitude reflects Anglo-American traditions of government and police in principle being a part of the community; in contrast, Italy, ruled by outsiders for so long, holds a stronger suspicion of government and those who give it information. In Italy, air travelers are told to watch their own luggage, but aren't asked to report if they see anything suspicious. The English language has no equivalent for the French *la delation*, the activity of informers (called *les corbeaux*, for crows). Nor do most Americans have recent historical memories of the well-developed systems for informing found in the former Soviet Union, East Germany, and the Nazi regime. When I taught in Austria, students were shocked to learn of the extent of American hotline outreach programs. They said citizens shouldn't be so willing to provide information to the state; it

was the job of the police to discover that information. The students were unaware of the irony that centuries earlier, one factor in the development of anonymous reporting systems (that often came with rewards) in Europe was the very failure of state agents to do their job honestly.

Obviously, police and citizens must cooperate on some level, and the ethos of community policing that has become more common in recent decades is generally positive: in a democracy, citizens should have input to police and a say in security. The need for transparency on the part of the state and for citizen involvement push toward weakening the borders between the police and the public, even as the protection of liberty pushes in the opposite direction.

As citizens, we want police secrecy to be restricted to settings where it's clearly necessary. Yet we want our personal information and private places and behavior to be protected from police, absent cause. The traditional informational flows seen after the reforms of Watergate appear to be undergoing alteration as more information on citizens becomes available to the saturating state and proportionally less from the state now flows to citizens. At least that is the case formally—ironically of course, as recent events such as the Snowden revelations show, there is also much more of the state's information to be leaked to the public. The larger the dyke and the more contained within it, the greater the likelihood of seepage and even bursting.

More than is the case for many organizations, police face conflicting needs to be both open as a means of democratic accountability and secret to protect operations, privacy, and confidentiality. The appropriate weighing of police transparency with police secrecy and of the privacy of personal information with the needs of the community is an eternal challenge for democratic societies.

In situations where the police would profit from crowd-sourced citizen input via search, analytical, and communication tools, the data should be welcomed, but performed under better controlled (both public and private) circumstances than at present. What procedures are needed to protect against masked, lynch mobs who are beyond conventional forms of accountability? Daren Brabham suggests using citizens in more directed ways, developing standards for what should count as evidence and providing the information to authorities rather than posting it online.¹¹ This could alleviate the problems seen in Boston, when two suspects were wrongly identified via social media (in one case, the erroneous identification was even reported in a newspaper). Daniel Trottier offers other suggestions in his case study of Internet crowdsourcing of CCTV surveillance.¹²

We value nonprofits, social movements, whistle-blowers, and the investigative journalism of a free press precisely because of their potential independence from the state and other powerful organizations and their ability to ferret out abuse. The democracy-sustaining idea of pluralism relies not only on the various branches of government but on a civil society. Our somewhat decentralized, anarchic net lends itself well to the discovery and communication of such findings by nonstate actors, whether they see themselves as working in parallel with the state or in opposition to it (WikiLeaks, Statewatch). But there's a need to better educate citizens about how and when it's appropriate to report information on violations and on the unwanted consequences of a rush to report, whether the reporting is on individuals or the state and to the state or to the public. The ambivalent and ambiguous role of informers and whistle-blowers needs to be seen

in its complexity and moral fluidity, depending on the context. Citizen responsibility must be responsibly done. And if police are to energetically seek citizen input, they must also have the ability to cull, protect, and use the information provided.

Problems seem more likely over these issues as we move from violations that have occurred to those that have not, from a missing person or a fugitive who has been tried in court to an identified suspect and thence to a "John Doe," unknown perpetrator; from serious crimes to misdemeanors; from suspect behavior to appearance or political beliefs; and from precise statements of what constitutes suspicion to vague requests to report. Anonymous (rather than layered pseudo-anonymous) forms of reporting and rewards are sometimes desirable, but they must be undertaken with great care, given their potential for undesirable consequences.

The risks of terror are clear, but they need to be put in perspective regarding the risks of institutionalizing a system of informing that overreaches and can have other significant social costs. Do efforts to mobilize the public as partners lead to increased feelings of security, and are they cost-effective relative to other uses of the resources? Or do they increase feelings of insecurity because of fear of the problem and constant reminders about it? Do they deter or simply lead to better-disguised plans for avoiding notice? The issue of precedent always looms large over any tool introduced for good purposes with the potential to be misused under changed historical circumstances. It isn't enough to justify it by saying the goal is good. We must also ask where it might lead and how it might be abused. The turn to citizens, particularly to private organizations, can result in the morally ambiguous area that Bob Hoogenboom calls "gray policing."¹³ In this gray, unregulated area,

police may delegate investigative tasks to private individuals, groups, and other countries not bound by the laws and policies that restrict state agents. In a climate where citizen cooperation is urged in general, authorities might simply be the beneficiaries of information from citizen volunteers, bound by neither the laws nor the policies that rein in state efforts. This blurring of the lines between the public and the private may help control crime but can violate the letter and spirit of laws intended to protect liberty.

Moreover, the creation of fear and the need for heightened citizen vigilance over unseen enemies (who could be anywhere and whose weapons take any form) can result in flooding overwhelmed police systems, not to mention unwarranted damage to reputations. The more permeable the borders between citizens' information and the police, the greater the threat to liberty. If we become too comfortable with the idea of reporting on every imaginable violation or problem, we risk diluting cooperation for more serious problems, overwhelming police resources, and introducing other problems.

But we also see another force involving, if not necessarily a clearer demarcation of those borders, at least the strengthening of civil society resources and institutions that parallel and supplement the limited resources of the state. Citizens acting independently can serve as a check on, and alternative to, the state and other large organizations, through decentralized, crowd-sourced, and other uses of the Internet. We need to be vigilant of those with power, so this force can be a healthy corrective. But what gives this tool its strength can also be a weakness, given issues of accountability that arise with its anonymous, de-territorialized nature.

We can add a line to the central paradox of any authority, so well put by James Madison in the *Federalist* (paper 51): “You must first enable the government to control the governed and in the next place, oblige it to control itself.” In a democracy, citizens too must be enabled to do both and in particular to control themselves in their efforts to control others. ■

References

1. L. Zedner, “Policing Before and After the Police: The Historical Antecedents of Contemporary Crime Control,” *British J. Criminology*, vol. 46, no. 1, 2006, pp. 78–96.
2. J. Reeves, “If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility,” *Surveillance and Society*, vol. 10, nos. 3 and 4, 2012, pp. 235–248.
3. C. Schneider and D. Trottier, “The 2011 Vancouver Riot and the Role of Facebook in Crowd Policing,” *BC Studies*, vol. 175, autumn 2012, pp. 57–72.
4. D. Montgomery, S. Horwitz, and M. Fisher, “Police, Citizens and Technology Factor into Boston Bombing Probe,” *Washington Post*, 20 Apr. 2013; http://articles.washingtonpost.com/2013-04-20/world/38693691_1_boston-marathon-finish-line-images.
5. A. Madrigal, “Hey Reddit, Enough Boston Bombing Vigilantism,” *The Atlantic*, 17 Apr. 2013; www.theatlantic.com/technology/archive/2013/04/hey-reddit-enough-boston-bombing-vigilantism/275062/.
6. J. Kang, “Should Reddit Be Blamed for the Spreading of a Smear?,” *New York Times Magazine*, 25 July 2013; www.nytimes.com/2013/07/28/magazine/should-reddit-be-blamed-for-the-spreading-of-a-smear.html?pagewanted=all.
7. M. Roth and J. Olson, “Hue and Cry,” *Historical Development Dictionary of Law Enforcement*, Greenwood Press, 2001.
8. E. Goffman, *The Presentation of Self in Everyday Life*, Doubleday, 1959.
9. M. Andrejevic, *iSpy Surveillance and Power in the Interactive Era*, Kansas Univ. Press, 2006.
10. A. Binder, “Double Murder Seen as Part of Man’s Quest to Kill Sex Offenders,” *New York Times*, 26 July 2013; www.nytimes.com/2013/07/27/us/2-targeted-sex-offender-to-be-killed-officials-say.html.
11. D. Brabham, “The Boston Marathon Bombings, 4Chan’s Think Tank, and a Modest Proposal for an Emergency Crowdsourced Investigation Platform,” 17 Apr. 2013; <http://culturedigitally.org/2013/04/boston-marathon-bombing-and-emergency-crowdsourced-investigation>.
12. D. Trottier, “Crowdsourcing CCTV Surveillance on the Internet,” to appear in *Information, Communication, and Society*, 2013.
13. R. Hoogenboom, *The Governance of Policing and Security: Ironies, Myths and Paradoxes*, Palgrave/MacMillan, 2010.

Gary T. Marx is professor emeritus of sociology at MIT. This article, written while he was a Braudel Fellow at the European University Institute, Fiesole, Italy, draws from material in his forthcoming book, *Windows into the Soul: Surveillance and Society in an Age of High Technology* (University of Chicago Press, forthcoming). Related material on topics such as citizen police patrols, soft surveillance, high policing, and informing are at www.garymarx.net.

 Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

Silver Bullet Security Podcast



In-depth interviews with security gurus. Hosted by Gary McGraw.



www.computer.org/security/podcasts
*Also available at iTunes

Sponsored by  digital